

TS Data

Transparent File Encryption

Introduction

TS Data is a token-based file encryption product for Windows NT and Windows 2000. TS Data allows for encryption of files, folders or drives, with an encryption key securely stored on a physical token, such as a smart card or USB token.

TS Data is a kernel-mode filter driver that once configured, encrypts data transparently to the user.

Configuration involves specifying files for encryption, which can be based on:

- File name
- File Type
- Folder
- Drive
- Mapped Drive.

TS Data is **CESG CAPS approved** at Baseline. Triple DES is supported by default, with AES or customer specific algorithms available.

Through easy to use configuration and management tools, the product allows the role of security administrator to be separated from general systems administration.

TS Data can be deployed stand-alone, or integrated with the **TS Security Suite**, providing access control, secured communications, and management software.

Increased Security

Token Key Storage

Flexible Encryption Policies

Removable Media Encryption

Data Encrypted Over The Network

Multiple Token Types Supported

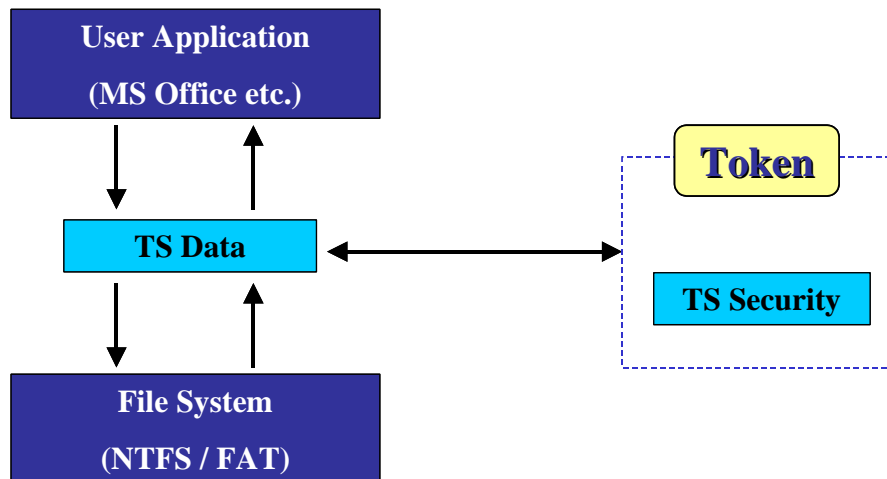
CESG Approved

Empowered Security Administrator

Integrated with TS Security Suite

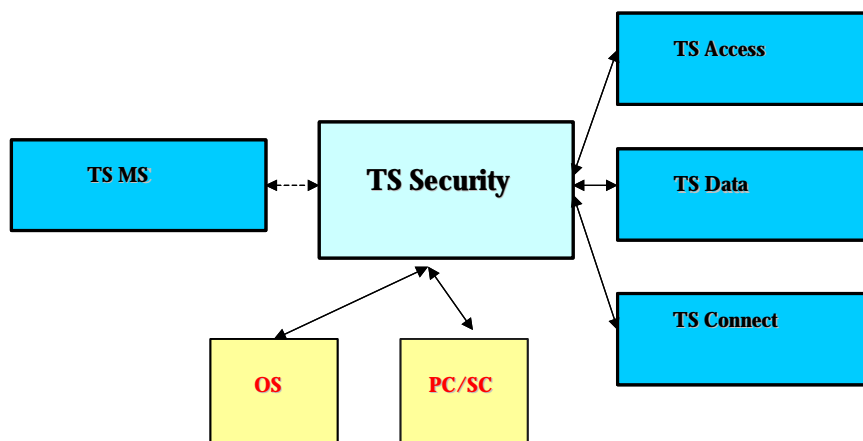


Overview



TS Data is implemented as a kernel mode filter driver, existing above the file system, and below user applications. TS Data intercepts all read or write operations made by applications. This allows transparent and efficient encryption or decryption of data as it is read from or written to disk.

The TS Data driver interacts with a set of core modules collectively known as **TS Security**. The core modules implement functionality common to all Topsoft security products, such as interacting with components of the operating system, or the smart card subsystem (PC/SC).



Secured Credentials

User credentials and encryption keys are stored securely on a token. Current token types supported include :

- Smart cards
- USB Tokens
- Touch Memories
- Virtual Tokens¹

Credentials are secured using the token's built-in security mechanisms, and are encrypted. Algorithms supported as standard include :

- 3DES
- Fireguard
- AES

However modular product design allows custom algorithm requirements to be supported.

TS Security uses a **Configuration Code** to determine which user credentials will be used for user authentication, and which credentials will be stored on the token. The Configuration Code may be supplied by the Topsoft supplier, or may be generated using the Configuration Code Wizard.

The code allows TS Security to be configured to use any combination of the following credentials for authentication :

- Domain
- Computer
- Username
- Password
- NT Security Identifier
- PIN number
- Security Clearance

The selected credentials are checked by TS Data and TS Security before access to or creation of encrypted data is allowed.

¹ Virtual tokens are software-only tokens that simulate physical tokens. These can be stored on floppy or the harddrive, removing the need for hardware installation.



File Encryption

The Topsoft Configuration Utility provides a user friendly interface for selection of files for encryption. Selection may be by a combination of :

File (s)

A specific file or group of files may be individually selected for encryption.

Folder (s)

A specific folder or group of folders may be individually selected for encryption, such that all files created with the folder will be encrypted.

File Type (s)

A specific file type such as *.doc may be selected for encryption.

Drive (s)

Specific drives may be selected for encryption. This includes floppy drives, allowing removable media to be encrypted.

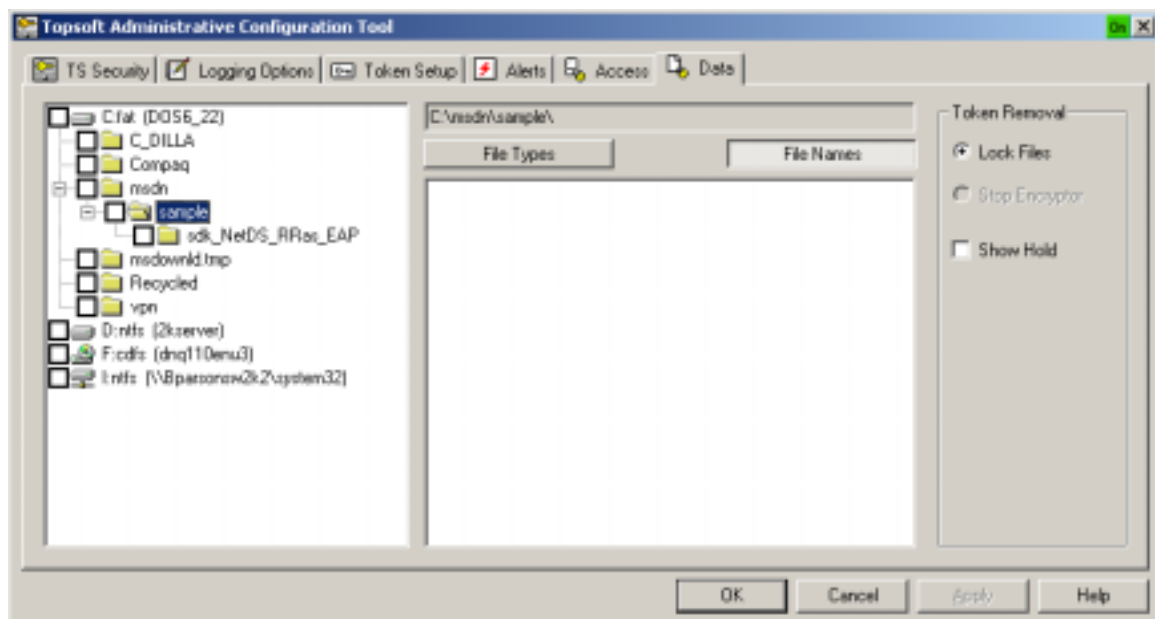
Note : certain system files can not be encrypted. Thus the entire system drive may not be selected for encryption

Mapped Drives

TS Data allows the selection of mapped drives. This would cause data transmitted across the network to be sent in encrypted form.

System Page file

The system page file can be selected for encryption.



Token Removal

TS Data will react to a token removal event by ceasing all cryptographic activity. The product can be configured to hide any sensitive data within open files by displaying a 'hold screen'.

Events

TS Security defines a set of security events relating to :

- The state of TS products
- The state of TS tokens
- Authentication events
- Security breaches

Combinations of these events can be selected for logging within any of the Windows event logs. Additionally, alerts can be generated for transmission to the TS Management System.

Utilities

Topsoft provide a set of utilities for use with TS Data. These include :

File Update Utility

The File Update Utility allows automatic re-encryption of encrypted files with a new encryption key following key change events.

Key Manager

The Key Manager Utility provides functionality for the secure storage and retrieval of encryption keys.

n-Crypt Products

TS Access	Access control
TS Data	File Encryption
TS MC	Management System
TS RAS	Secure dial-up
TS SafeFile	Drag & Drop Encryptor
TS SafeDoc	Secure package

N-Crypt Limited

Berkshire House
252-256 Kings Road
Reading
Berkshire
RG1 4HP

Tel 01189 533733
Email: security@n-crypt.co.uk
HTTP: www.n-crypt.co.uk

